UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/693,605	10/20/2000	Ashraf Madoukh	15247.6	8437

7590 09/01/2004

Kyle L. Elliott
Blackwell Sanders Peper Martin, LLP
2300 Main Street
Suite 1000
Kansas City, MO 64108

EXAMINER	
SHERKAT, AREZOO	

ART UNIT	PAPER NUMBER
2131	13

DATE MAILED: 09/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/693,605	MADOUKH ET AL.	
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 October 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-120* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-120* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 October 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2,3,8,12*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-120 are presented for examination.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1, 6-8, 10, 17-21, 26-28, 40-44, 80, and 96-99 are rejected under 35 U.S.C. 102(e) as being anticipated by Ho, (U.S. Patent No. 6,148,342 and Ho hereinafter).

Regarding claims 1, 6-8, 10, 17-21, 26-28, 40-44, 80, and 96-99, Ho discloses a computer readable medium containing a database structure for storage of encrypted data, the database structure comprising: at least one data entity encrypted by at least

one encryption key, the data entity having at least one searchable attribute, and at least one encryption key identification in association with the data entity and corresponding to the encryption key (Col. 3, lines 37-67 and Col. 4, lines 1-58).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2, 5, 11, 13-16, 22-25, 29-36, 45-50, 66, and 81-85 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ho, (U.S. Patent No. 6,148,342 and Ho hereinafter), in view of Matyas et al., (U.S. Patent No. 4,757,534 and Matyas hereinafter).

Regarding claims 2, 5, 11, 13-16, 22-25, 29-36, 45-50, 66, 78, and 81-85, Ho does not expressly disclose wherein the at least one encryption key identification is encrypted by a system key.

However, Matyas discloses wherein the at least one encryption key identification (i.e., file key, KF) is encrypted by a system key (i.e., key, KP), and the database structure further comprises a system key common name (i.e., card number) corresponding to the system key, and the system key common name being stored in

association with the data entity (Col. 10, lines 8-67 and Col. 11-12, lines 1-67 and Col. 13, lines 1-20).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Ho with the teachings of Matyas because it would allow to include wherein the at least one encryption key identification (i.e., file key, KF) is encrypted by a system key (i.e., key, KP) with the motivation to allow the user to decrypt and execute the program on any computer having a properly implemented and initialized encryption feature (Matyas, Col. 3, lines 9-15).

Regarding claims 51-52, 55-57, 64, 88-91, and 93-95, Ho does not expressly disclose further comprising checking for expiration of the system key, and upon expiration of the system key, discontinuing use of the system key and generating and using a new system key.

However, Matyas discloses further comprising checking for expiration of the system key, and upon expiration of the system key, discontinuing use of the system key and generating and using a new system key (Col. 9, lines 22-41).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Ho with the teachings of Matyas because it would allow to include further comprising checking for expiration of the system key, and upon expiration of the system key, discontinuing use of the system key and generating and using a new system key with the motivation to prevent another

copy of the encrypted program on a different diskette to be decrypted and executed (Matyas, Col. 9, lines 22-41).

Regarding claims 111-120, Ho discloses an encryption and decryption method for encrypting and decrypting data, the method comprising: encrypting data with an encryption key having an encryption key identification (Col. 3, lines 37-67 and Col. 4, lines 1-58).

Ho does not expressly disclose encrypting the encryption key identification with a system key having a system key common name.

However, Matyas discloses encrypting the encryption key identification with a system key having a system key common name (Col. 9, lines 22-41).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Ho with the teachings of Matyas because it would allow to include encrypting the encryption key identification with a system key having a system key common name with the motivation to allow the user to decrypt and execute the program on any computer having a properly implemented and initialized encryption feature (Matyas, Col. 3, lines 9-15).

Claims 3-4, 9, 37-39, 53, and 86-87 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ho, (U.S. Patent No. 6,148,342 and Ho hereinafter) and Matyas et al., (U.S. Patent No. 4,757,534 and Matyas hereinafter), in view of Kaufman et al., (U.S. Patent No. 5,764,772 and Kaufman hereinafter).

Regarding claims 3-4, 9, 37-39, 53, and 86-87, Ho or Matyas does not expressly disclose wherein the system key common name is hashed, and the data structure further comprising a system key common name hash value stored in association with the system common name.

However, Kaufman discloses wherein the system key common name is hashed, and the data structure further comprising a system key common name hash value stored in association with the system common name (Col. 8, lines 20-67 and Col. 9, lines 1-63).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Ho and Matyas with the teachings of Kaufman because it would allow to include wherein the system key common name is hashed, and the data structure further comprising a system key common name hash value stored in association with the system common name with the motivation to make it impossible to make an undetected modification to the encrypted key field once the encrypted message was generated (Kaufman, Col. 10, lines 20-37).

Claims 12, 54, 58-63, 65, 67-79, 92, and 100-110 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ho, (U.S. Patent No. 6,148,342 and Ho hereinafter) and Matyas et al., (U.S. Patent No. 4,757,534 and Matyas hereinafter), in view of

Kaufman et al., (U.S. Patent No. 5,764,772 and Kaufman hereinafter), in further view of Alegre et al., (U.S. Patent No. 6,199,113 and Alegre hereinafter).

Regarding claims 54, 58-59, 70-79, and 100-104, Ho discloses a computer readable medium containing a database structure for storage of encrypted data, the database structure comprising: at least one data entity encrypted by at least one encryption key, the data entity having at least one searchable attribute, and at least one encryption key identification in association with the data entity and corresponding to the encryption key (Col. 3, lines 37-67 and Col. 4, lines 1-58).

Ho or Matyas or Kaufman does not expressly disclose requesting a data manipulation using a searchable attribute, searching for matches to the searchable attribute, searching for the system key common name using the system key hash value, searching for the system key using the system key common name, decrypting the encryption key identification with the system key, searching for the encryption key using the encryption key identification, and decrypting the data entity with the encryption key.

However, Alegre discloses further comprising:

requesting a data manipulation using a searchable attribute, searching for matches to the searchable attribute, searching for the system key common name using the system key hash value, searching for the system key using the system key common name, decrypting the encryption key identification with the system key, searching for the encryption key using the encryption key identification, and decrypting the data entity with the encryption key (Col. 2, lines 12-67 and Col. 6, lines 23-50).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Ho and Matyas and Kaufman with the teachings of Alegre because it would allow to include requesting a data manipulation using a searchable attribute, searching for matches to the searchable attribute, searching for the system key common name using the system key hash value, searching for the system key using the system key common name, decrypting the encryption key identification with the system key, searching for the encryption key using the encryption key identification, and decrypting the data entity with the encryption key with the motivation to allow access y users on the Internet in a controlled and secure manner (Alegre, Col. 2, lines 30-35).

Regarding claims 60-62, and 92, Ho or Matyas does not expressly disclose further comprising generating a new encryption key for each user action.

However, Alegre discloses further comprising generating a new encryption key for each user action (Col. 5, lines 7-67 and Col. 6, lines 1-50).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Ho and Matyas with the teachings of Alegre because it would allow to include generating a new encryption key for each user action with the motivation to allow access y users on the Internet in a controlled and secure manner (Alegre, Col. 2, lines 30-35).

Regarding claims 12, 63 and 65, Ho does not expressly disclose wherein the data entity and encryption key identification are stored in a first database, and further comprising storing the encryption key in a second database.

However, Alegre discloses wherein the data entity and encryption key identification are stored in a first database, and further comprising storing the encryption key in a second database (Col. 4, lines 8-67 and Col. 5, lines 1-7).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Ho with the teachings of Alegre because it would allow to include wherein the data entity and encryption key identification are stored in a first database, and further comprising storing the encryption key in a second database with the motivation to allow access y users on the Internet in a controlled and secure manner (Alegre, Col. 2, lines 30-35).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Halter et al., (U.S. Patent No. 5,319,705),

Harrison, (U.S. Patent No. 5,870,468),

Brundrett et al., (U.S. Patent No. 6,249,866),

Margolus et al., (U.S. Publication No. 2004/0143745).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (703) 305-8749. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

A. Sherkat

Arezoo Sherkat
Patent Examiner
Art Group 2131
Aug. 26, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100